LISTING OF THE CLAIMS

1-15. Canceled.

16. (Currently amended) A process for use in identifying a customer computer involved in an online transaction via a merchant web site between a customer using a customer browser operating on said customer computer and a merchant who operates said merchant web site, in order to monitor for possible fraudulent transactions using the computer, said method comprising the steps of:

said merchant web site providing to said customer browser a redirect script request within a transaction form of said merchant web site, wherein said redirect script causes said customer browser to communicate to an archiver web site of a machine data archiving service an electronic request for a machine data collection script;

said archiver web site returning said machine data collection script to said customer browser along with a transaction identification string, wherein said machine data collection script causes said customer browser processing said machine data collection script to cause said customer browser to query said customer computer for a machine fingerprint of said customer computer, wherein said machine fingerprint comprises a hashed attribute string associated with one or more attributes of said customer computer, and wherein said machine data collection script causes said customer browser to communicate said machine fingerprint and said transaction identification string to said archiver web site, and said archiver web site storing said machine fingerprint and said transaction identification string in a machine data profile as an archiver record;

wherein said machine data collection script also causes said customer browser to write said transaction identification string into said transaction form; [[and]]

said merchant web site receiving from said customer browser customer identification information with said transaction form to thereby comprise a transaction record, and storing the transaction record with the transaction identification string as a merchant record;

whereby said transaction identification string associates said transaction record with said machine fingerprint; and

monitoring for possible fraudulent transactions, wherein said monitoring is based at least in part on said machine fingerprint.

17. (Previously presented) A process as set forth in claim 16 wherein said machine data collection script causes said customer browser to communicate said machine fingerprint and said transaction identification string along with a conventional hypertext transfer protocol (HTTP) header, and wherein the process further comprises the step of said archiver service additionally storing said HTTP header in association with said machine data profile.

18. (Previously presented) A process as set forth in claim 16 further comprising said machine data collection script querying said customer browser for a configuration setting thereof.

19. (Previously presented) A process as set forth in claim 16 wherein said script causes said customer browser to provide a plurality of configuration settings, and to form an attribute string from said plurality of configuration settings, and to process said attribute string to form said machine fingerprint of said customer computer.

20. (Previously presented) A process as set forth in claim 19 wherein said script performs a hashing function on said attribute string to form said machine fingerprint.

21. (Previously presented) A process as set forth in claim 16 wherein said redirect script causes customer computer to access said merchant web site by way of a proxy, and to communicate said machine fingerprint and said transaction identification string to said archiver web site using a protocol which bypasses said proxy.

22. (Previously presented) A process as set forth in claim 16 wherein said machine data collection script causes said customer browser to communicate said machine fingerprint to said archiver web site using a protocol other than HTTP.

23. (Previously presented) A process as set forth in claim 16 wherein said customer computer comprises a digital clock, and wherein said script causes said customer browser to query said

clock for a time value, and to send said time value to said archiver web site along with said machine fingerprint.

24-26. Canceled.

27. (Currently Amended) ~~A process as in claim 16, further comprising:~~ A process for use in identifying a customer computer involved in an online transaction via a merchant web site between a customer using a customer browser operating on said customer computer and a merchant who operates said merchant web site, in order to monitor for possible fraudulent transactions using the computer, said method comprising the steps of:

said merchant web site providing to said customer browser a redirect script request within a transaction form of said merchant web site, wherein said redirect script causes said customer browser to communicate to an archiver web site of a machine data archiving service an electronic request for a machine data collection script;

said archiver web site returning said machine data collection script to said customer browser along with a transaction identification string, wherein said machine data collection script causes said customer browser processing said machine data collection script to cause said customer browser to query said customer computer for a machine fingerprint of said customer computer, wherein said machine fingerprint comprises a hashed attribute string associated with one or more attributes of said customer computer, and wherein said machine data collection script causes said customer browser to communicate said machine fingerprint and said transaction identification string to said archiver web site, and said archiver web site storing said machine fingerprint and said transaction identification string in a machine data profile as an archiver record;

wherein said machine data collection script also causes said customer browser to write said transaction identification string into said transaction form;

said merchant web site receiving from said customer browser customer identification information with said transaction form to thereby comprise a transaction record, and storing the transaction record with the transaction identification string as a merchant record;

whereby said transaction identification string associates said transaction record with said machine fingerprint; and

a qualified party accessing said archiver web site to examine said machine fingerprint and said transaction identification string along with other machine fingerprints and transaction identification strings in order to determine evidence of a pattern of suspicious behavior by a customer associated with said transaction identification string.

28. (New) A process for use in identifying a customer computer involved in an online transaction via a merchant web site between a customer using a customer browser operating on said customer computer and a merchant who operates said merchant web site, in order to monitor for possible fraudulent transactions using the computer, said method comprising the steps of:

said merchant web site providing to said customer browser a redirect script request within a transaction form of said merchant web site, wherein said redirect script causes said customer browser to communicate to an archiver web site of a machine data archiving service an electronic request for a machine data collection script;

said archiver web site returning said machine data collection script to said customer browser along with a transaction identification string, wherein said machine data collection script causes said customer browser processing said machine data collection script to cause said customer browser to query said customer computer for a machine fingerprint of said customer computer, wherein said machine fingerprint comprises a hashed attribute string associated with one or more attributes of said customer computer, and wherein said machine data collection script causes said customer browser to communicate said machine fingerprint and said transaction identification string to said archiver web site, and said archiver web site storing said machine fingerprint and said transaction identification string in a machine data profile as an archiver record;

wherein said machine data collection script also causes said customer browser to write said transaction identification string into said transaction form;

said merchant web site receiving from said customer browser customer identification information with said transaction form to thereby comprise a transaction record, and storing the transaction record with the transaction identification string as a merchant record;

whereby said transaction identification string associates said transaction record with said machine fingerprint; and

analyzing information related to said transaction record and said machine fingerprint to monitor whether said online transaction is fraudulent.

29. (New) A process for use in identifying a customer computer involved in an online transaction via a merchant web site between a customer using a customer browser operating on said customer computer and a merchant who operates said merchant web site, in order to monitor for possible fraudulent transactions using the computer, said method comprising the steps of:

said merchant web site providing to said customer browser a redirect script request within a transaction form of said merchant web site, wherein said redirect script causes said customer browser to communicate to an archiver web site of a machine data archiving service an electronic request for a machine data collection script;

said archiver web site returning said machine data collection script to said customer browser along with a transaction identification string, wherein said machine data collection script causes said customer browser processing said machine data collection script to cause said customer browser to query said customer computer for a machine fingerprint of said customer computer, wherein said machine fingerprint comprises a hashed attribute string associated with one or more attributes of said customer computer, and wherein said machine data collection script causes said customer browser to communicate said machine fingerprint and said transaction identification string to said archiver web site, and said archiver web site storing said machine fingerprint and said transaction identification string in a machine data profile as an archiver record;

wherein said machine data collection script also causes said customer browser to write said transaction identification string into said transaction form;

said merchant web site receiving from said customer browser customer identification information with said transaction form to thereby comprise a transaction record, and storing the transaction record with the transaction identification string as a merchant record;

whereby said transaction identification string associates said transaction record with said machine fingerprint; and

examining information related to said transaction record and said machine fingerprint along with information related to at least one other transaction identification string in order to monitor for possible fraudulent transactions.

30. (New) A process for use in identifying a customer computer involved in an online transaction via a merchant web site between a customer using a customer browser operating on said customer computer and a merchant who operates said merchant web site, in order to monitor for possible fraudulent transactions using the computer, said method comprising the steps of:

said merchant web site providing to said customer browser a redirect script request within a transaction form of said merchant web site, wherein said redirect script causes said customer browser to communicate to an archiver web site of a machine data archiving service an electronic request for a machine data collection script;

said archiver web site returning said machine data collection script to said customer browser along with a transaction identification string, wherein said machine data collection script causes said customer browser processing said machine data collection script to cause said customer browser to query said customer computer for a machine fingerprint of said customer computer, wherein said machine fingerprint comprises a hashed attribute string associated with one or more attributes of said customer computer, and wherein said machine data collection script causes said customer browser to communicate said machine fingerprint and said transaction identification string to said archiver web site, and said archiver web site storing said machine fingerprint and said transaction identification string in a machine data profile as an archiver record;

wherein said machine data collection script also causes said customer browser to write said transaction identification string into said transaction form;

said merchant web site receiving from said customer browser customer identification information with said transaction form to thereby comprise a transaction record, and storing the transaction record with the transaction identification string as a merchant record;

whereby said transaction identification string associates said transaction record with said machine fingerprint; and

accessing said archiver web site to examine information related to said machine fingerprint and said transaction identification string along with other machine fingerprints and transaction identification strings in order to monitor for possible fraudulent transactions.